

CSM TACACSとISEの統合

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[認証手順](#)

[ISE の設定](#)

[CSMの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、管理者ユーザがTACACS+プロトコルで認証できるように、Cisco Security Manager(CSM)とIdentity Services Engine(ISE)を統合する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Security Manager(CSM)
- Identity Services Engine(ISE)。
- TACACS+プロトコル。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CSMサーババージョン4.22
- ISE バージョン 3.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

デフォルトでは、Cisco Security Manager(CSM)はCiscoverksという認証モードを使用してユーザをローカルで認証および許可し、中央集中型の認証方式を使用するために、TACACSプロトコルを使用してCisco Identity Service Engineを使用できます。

設定

ネットワーク図



認証手順

ステップ1:管理ユーザのクレデンシャルを使用してCSMアプリケーションにログインします。

ステップ2: 認証プロセスがトリガーされ、ISEがローカルまたはActive Directoryを介してクレデンシャルを検証します。

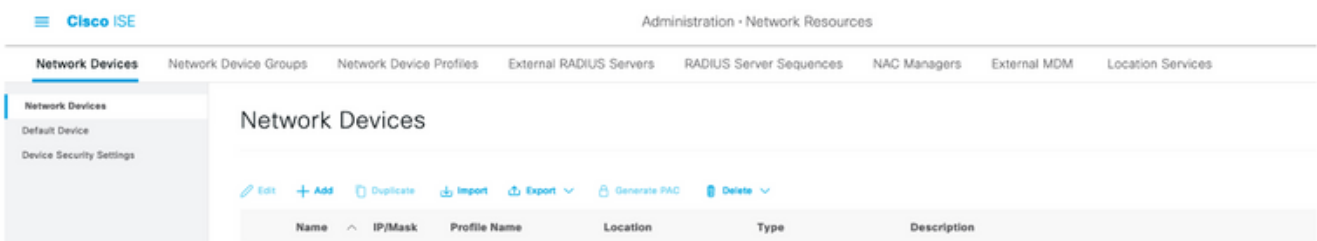
ステップ3: 認証が成功すると、ISEはCSMへのアクセスを許可する許可パケットを送信します。

ステップ4:CSMはユーザ名とローカルユーザロールの割り当てをマッピングします。

ステップ5:ISEは成功した認証のライブログを表示します。

ISE の設定

ステップ1:3回線アイコンを選択します  左上に表示され、[Administration] > [Network Resources] > [Network Devices]に移動します。



ステップ2:+Addボタンを選択して、Network Access Device NameとIP Addressに適切な値を入力し、次にTACACS Authentication Settingsチェックボックスを確認し、共有秘密を定義します。「送信」ボタンを選択します。

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

* Name: CSM432

Description:

IP Address: 10.88.243.42 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations [Set To Default](#)

IPSEC: Is IPSEC Device [Set To Default](#)

Device Type: All Device Types [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret: [Show](#)

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

[Submit](#) [Cancel](#)



ステップ3:3つの回線アイコンを選択します
[Identity Management] > [Groups]に移動します。

左上隅に表示され、[Administration] >

☰ Cisco ISE Administration • Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

EQ

< [Icon] [Icon]

> Endpoint Identity Groups

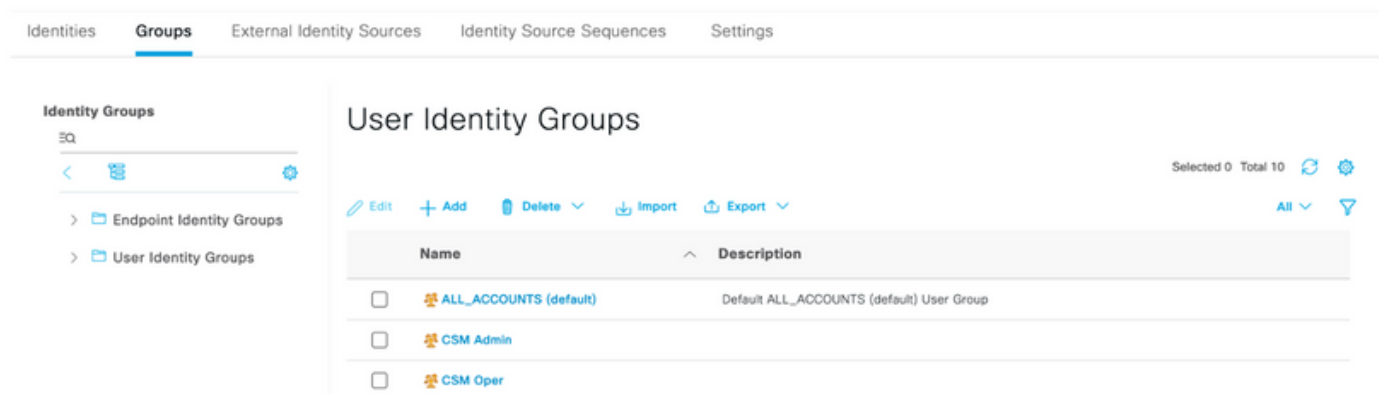
> **User Identity Groups**

User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

ステップ4:[User Identity Groups]フォルダに移動し、[+Add]ボタンを選択します。名前を定義し、「送信」ボタンを選択します。



The screenshot shows the 'User Identity Groups' management page. The navigation bar includes 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The left sidebar shows 'Identity Groups' with a search bar and a tree view containing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups' and shows a table with columns 'Name' and 'Description'. The table lists three groups: 'ALL_ACCOUNTS (default)', 'CSM Admin', and 'CSM Oper'. Above the table are buttons for 'Edit', '+ Add', 'Delete', 'Import', and 'Export'. The top right corner shows 'Selected 0 Total 10' and a refresh icon.

注：この例では、CSM AdminおよびCSM Oper Identityグループを作成します。CSMの管理ユーザのタイプごとに、ステップ4を繰り返すことができます



ステップ5:3回線アイコンを選択します [Administration] > [Identity Management] > [Identities]に移動します。[+Add]ボタンを選択し、ユーザ名とパスワードを定義してから、ユーザが属するグループを選択します。この例では、csmadminユーザとcsmoperユーザを作成し、それぞれCSM AdminおよびCSM Operグループに割り当てます。

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users List > csmadmin

Network Access User

* Name csmadmin

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-linear Password

* Login Password *****

These Password *****

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds 2021-05-15 (yyyy-mm-dd)

User Groups

CSM Admin

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Status	Name	Description	First Name	Last Name	Email Address	User Identity Grou...	Ad...
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled csmadmin					CSM Admin	
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled csmoper					CSM Oper	



ステップ6:選択 [Administration] > [System] > [Deployment]に移動します。ホスト名ノードを選択し、デバイス管理サービスを有効にします

Hostname	Personas	Role(s)	Services	Node Status
Ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE...	✔

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

注：分散導入の場合は、TACACS要求を処理するPSNノードを選択します

ステップ7:3つの回線アイコンを選択し、[Administration] > [Device Administration] > [Policy Elements]に移動します。[Results] > [TACACS Command Sets]に移動します。[+ Add]ボタンを選択して、コマンドセットの名前を定義し、[Permit any command that is not listed below]チェックボックスをオンにします。Submit を選択します。

Cisco ISE Work Centers - Device Administration Evaluation Mode 39 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets More

TACACS Command Sets > New Command Set

Name: Permit all

Description:

Commands: Permit any command that is not listed below

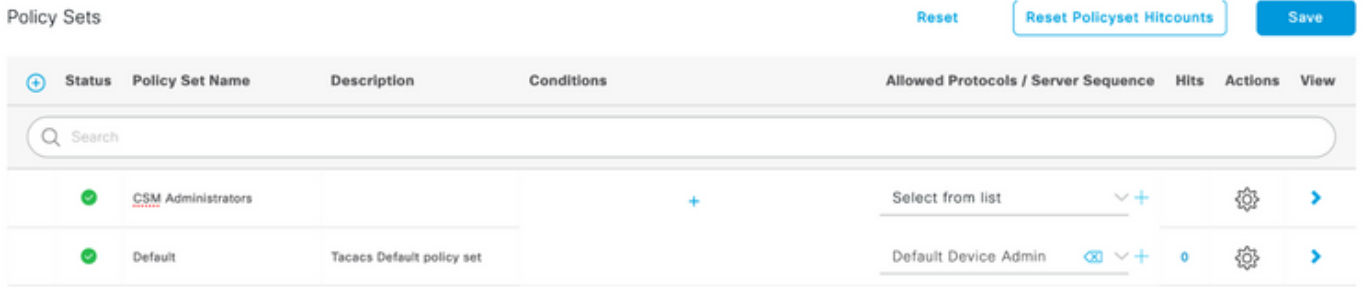
+ Add Trash Edit Move Up Move Down

Grant	Command	Arguments
No data found.		

Cancel Submit

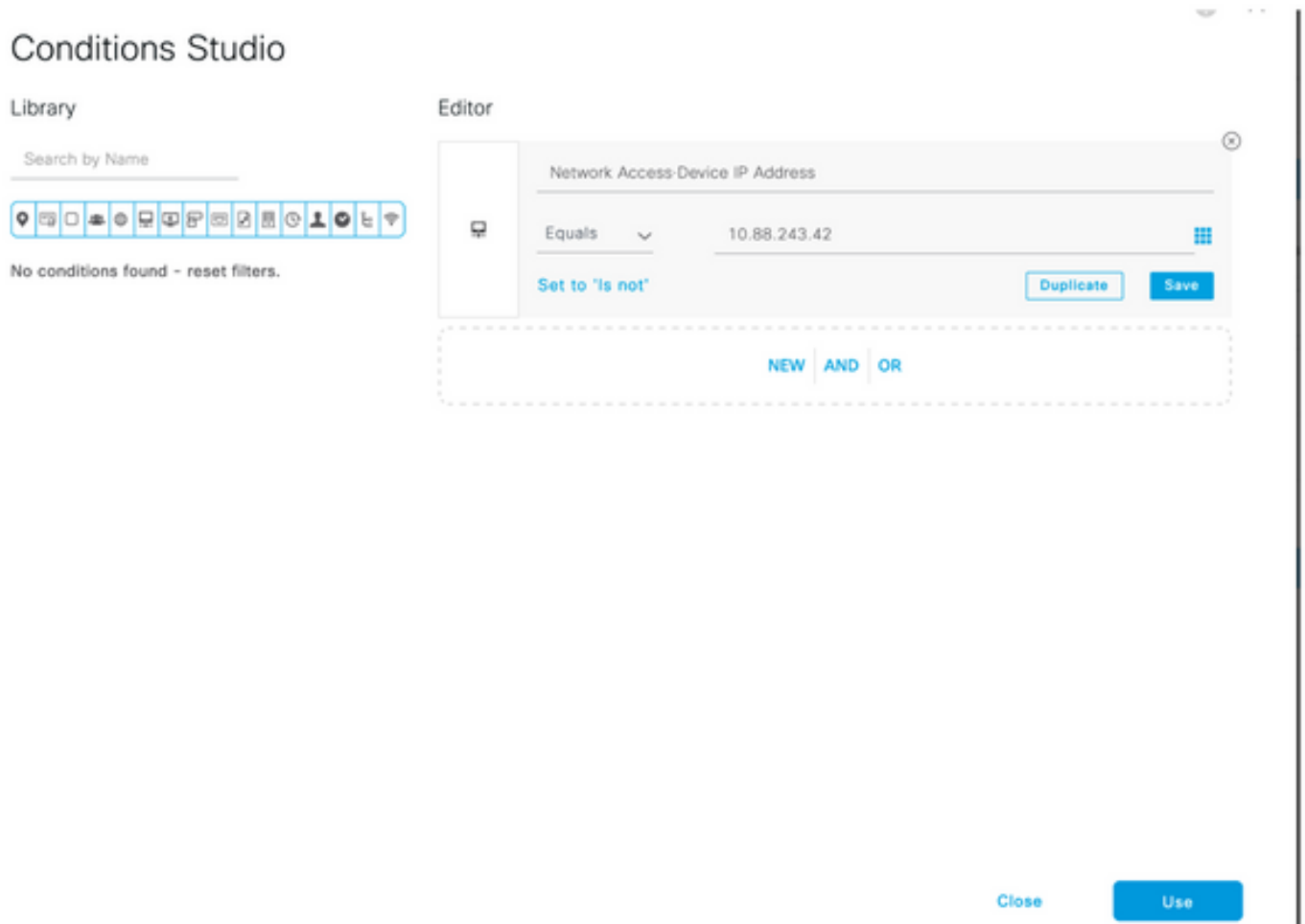
ステップ8：左上の3つの回線アイコンを選択し、[Administration] > [Device Administration] >

[Device Admin Policy Sets]に移動します。選択 [Policy Sets title]の下にある名前を定義し、中央の[+]ボタンを選択して新しい条件を追加します。



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CSM Administrators		+	Select from list	+	⚙️	➔
●	Default	Tacacs Default policy set		Default Device Admin	0	⚙️	➔

ステップ9:[Condition]ウィンドウで、[add a attribute]を選択し、[Network Device Icon]、[Network access device IP address]の順に選択します。 [Attribute Value]を選択し、CSM IPアドレスを追加します。 [Use once done]を選択します。



Conditions Studio

Library

Search by Name

No conditions found - reset filters.

Editor

Network Access-Device IP Address

Equals 10.88.243.42

Set to 'is not'

Duplicate Save


NEW AND OR


Close Use

ステップ10:[allow protocols]セクションで、[Device Default Admin]を選択します。 [保存 (Save)]を選択します。

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CSM 4.22		Network Access-Device IP Address EQUALS 10.88.243.42	Default Device Admin	0		

ステップ11:右矢印を選択します  アイコンをクリックします。

ステップ12:選択  [Authentication Policy title]の下にある名前を定義し、中央の[+]を選択して新しい条件を追加します。[条件]ウィンドウで、[属性の追加]を選択し、[ネットワークデバイスアイコン]を選択し、次に[ネットワークアクセスデバイスのIPアドレス]を選択します。 [Attribute Value]を選択し、CSM IPアドレスを追加します。完了したら[使用]を選択します

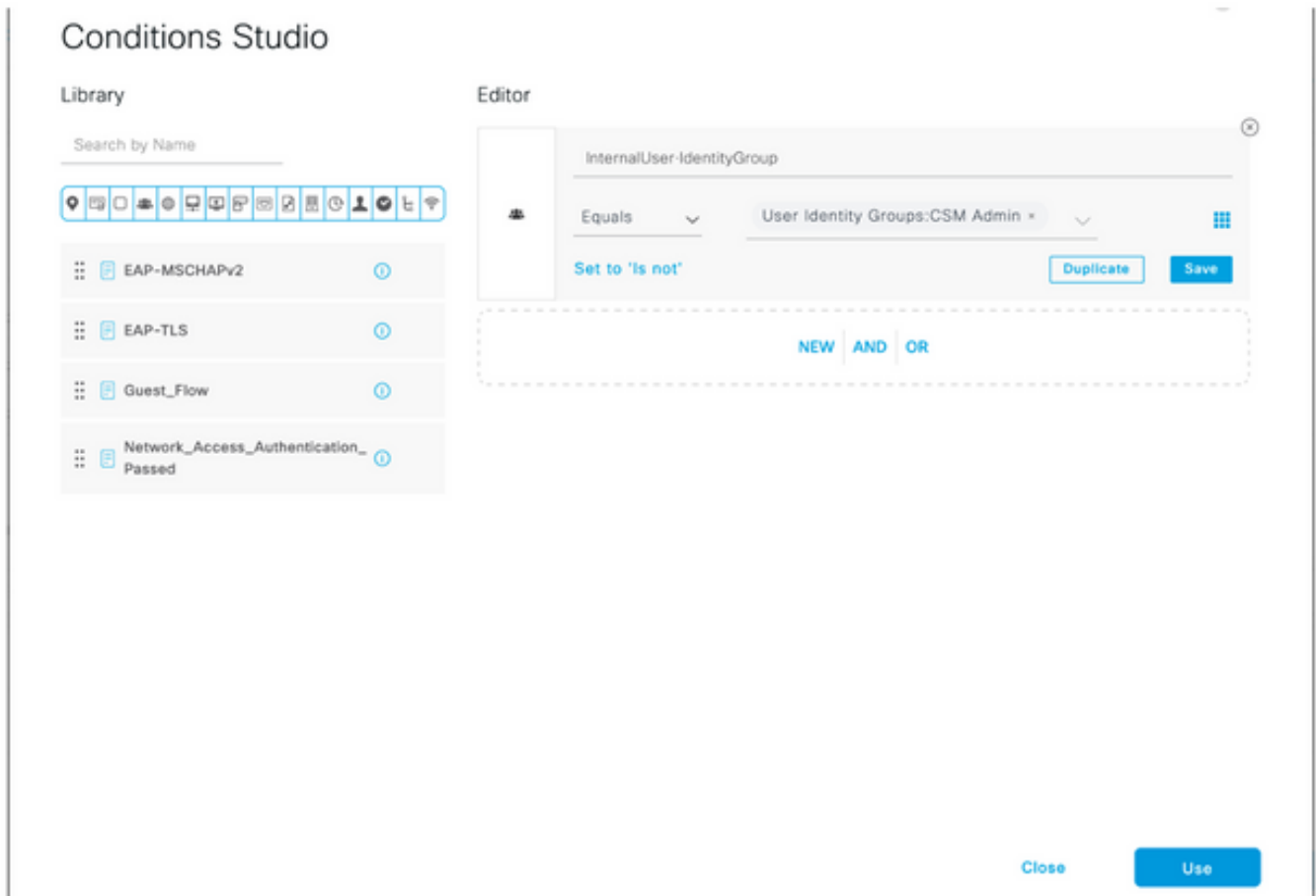
ステップ13:IDストアとして[内部ユーザー]を選択し、[保存]を選択します

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	CSM Authentication	Network Access-Device IP Address EQUALS 10.88.243.42	Internal Users		Options

注：ISEがActive Directoryに参加している場合、IDストアをADストアに変更できます。

ステップ14:選択  認可ポリシーのタイトルの下にある名前を定義し、中央の+ボタンを選択して新しい条件を追加します。[Condition]ウィンドウで、[add an attribute]を選択し、[Identity Group]アイコンを選択し、続いて[Internal User:Identity Group。 [CSM Admin Group]を選択し、[Use]を選択します。



ステップ15:[Command Set]で、[Step 7で作成したすべてのコマンドセットを許可]を選択し、[Save]を選択します

CSM Operグループに対してステップ14と15を繰り返します

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions	
			Command Sets	Shell Profiles				
✓	CSM Oper	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	Permit all ×	+	Select from list	+	0	⚙️
✓	CSM Admin	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	Permit all ×	+	Select from list	+	0	⚙️
✓	Default		DenyAllCommands ×	+	Deny All Shell Profile	+	0	⚙️

ステップ 16 (オプション) : 左上にある3つの回線アイコンを選択し、[Administration] > [System] > [Maintenance] > [Repository]を選択して、[+Add]を選択し、トラブルシューティングのためにTCPダンプファイルを保存するリポジトリを追加します。

ステップ 17 (オプション) : リポジトリ名、プロトコル、サーバ名、パス、およびクレデンシャルを定義します。完了したら[送信]を選択します。

Deployment Licensing Certificates Logging **Maintenance** Upgrade Health Checks Backup [Click here to do visibility setup Do not show this again.](#)

Patch Management

Repository

Operational Data Purging

[Repository List](#) > [Add Repository](#)

Repository Configuration

* Repository Name

* Protocol

Location

* Server Name

* Path

Credentials

* User Name

* Password

CSMの設定

ステップ1：ローカル管理者アカウントでCisco Security Managerクライアントアプリケーションにログインします。メニューから[Tools] > [Security Manager Administration]に移動します

Cisco Security Manager
Version 4.22.0 Service Pack 1

Server Name

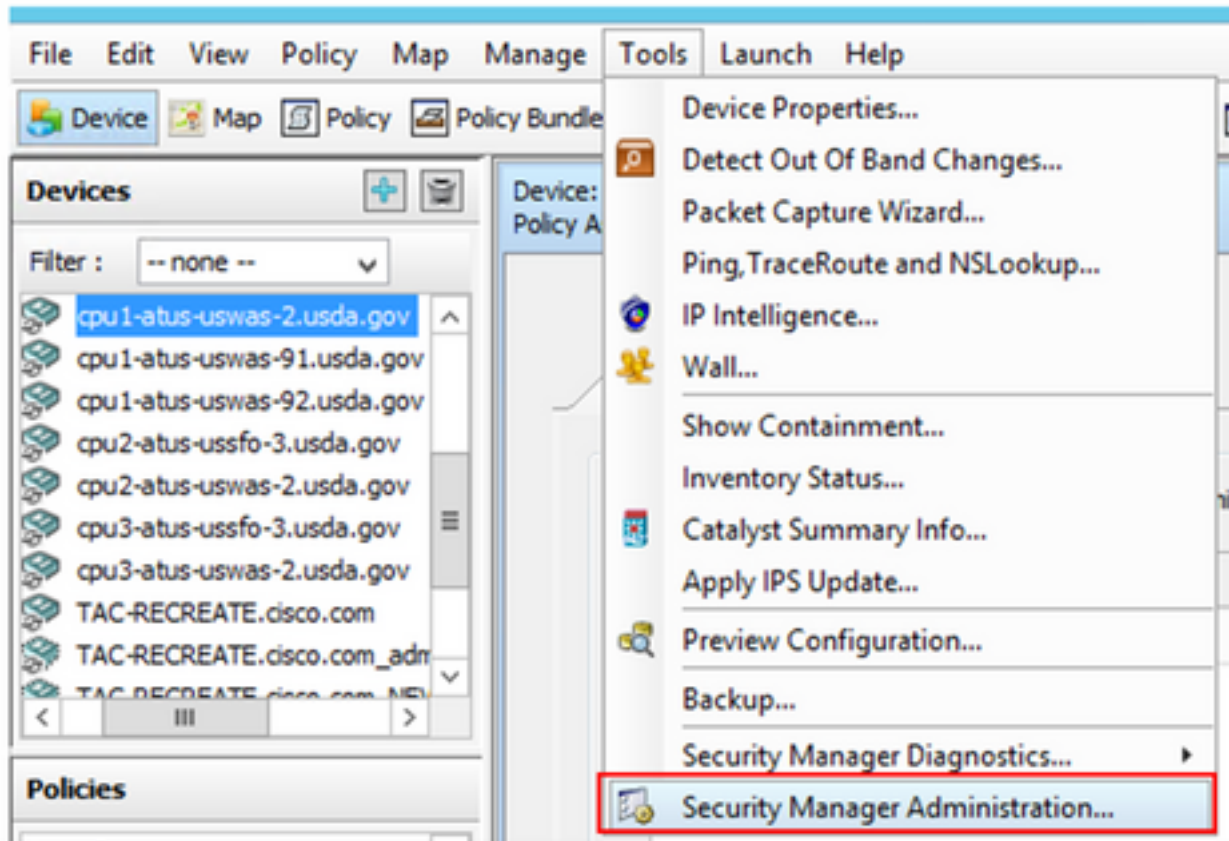
Username

Password

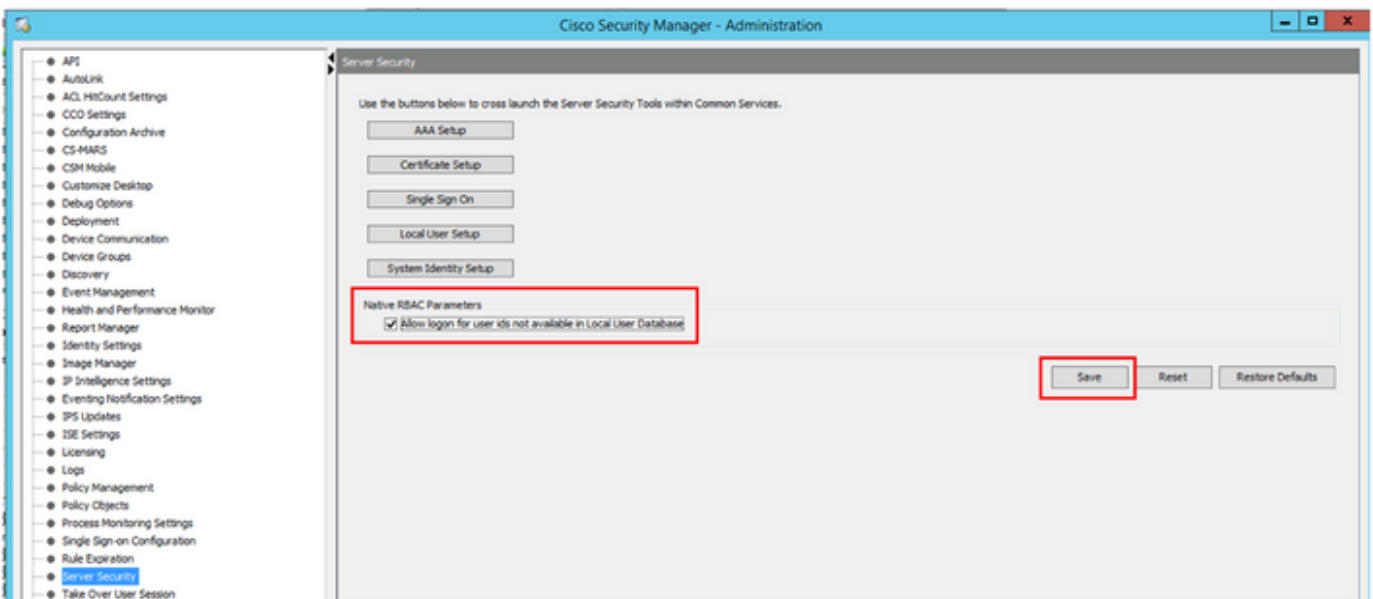
Default View

[Login](#) [Help](#)

© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.



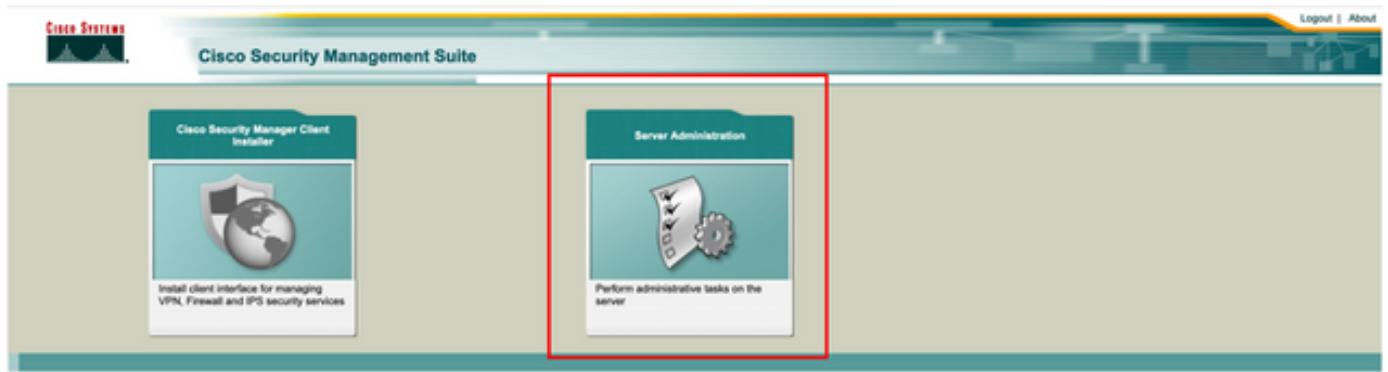
ステップ2:[Native RBAC Parameters]の下のボックスをオンにします。[保存して閉じる]を選択します



ステップ3：メニューから[File] > [Submit]を選択します。[File] > [Submit]を選択します。

注：設定変更の場合は、すべての変更を保存する必要があります。これらの変更を送信して展開する必要があります。

ステップ4:CSM Management UIに移動し、https://<enter_CSM_IP_Address>と入力してServer Administrationを選択します。



注：手順4～7は、ISEで定義されていないすべての管理者のデフォルトロールを定義する手順を示しています。次の手順はオプションです。

ステップ5：認証モードがCiscoWorks Localに設定されていることを確認し、Online userIDはCSMで作成されたローカル管理者アカウントです。

Common Services Home

Version: 4.2.2

Last Updated: Sat Apr 17 14:11:20 PDT 2021

Security		Backup		Recently Completed Jobs					
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ID	Job Type	Status	Description	Completed At	
Authorization Mode	CiscoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1369	SystemCheckUtility	Succeeded	SysCheckTest	Fri Apr 16 05:00:58 PDT 2021	
Single Sign-on Mode	Standalone	Recent Backup Status	Not found or unable to detect	1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021	
				1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021	
				1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021	
				1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021	
				1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021	
				1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 10 05:00:56 PDT 2021	

System Tasks	Online Users	Management Tasks	Reports
Local User Setup Multi-Server Trust Management Configure Single Sign-On AAA Mode Setup	Number of Online users: 1 Online User ID(s): admin Send Message	Schedule Backup Check for Software Updates Check for Device Updates Collect Server Information	Permission Report Log File Status Process Status System Audit Log

ステップ6:[Server]に移動し、[Single-Server Management]を選択します



Common

Auto R

Authentica

Authorizat

Single Sig

Local Use

Multi-Serv

Configure

AAA Mode Setup

Security

Single-Server Management

Multi-Server Trust Management

Cisco.com Connection Management

AAA Mode Setup

Admin

Processes

Backup

Log Rotation

Collect Server information

Selftest

Notify Users

Job Browser

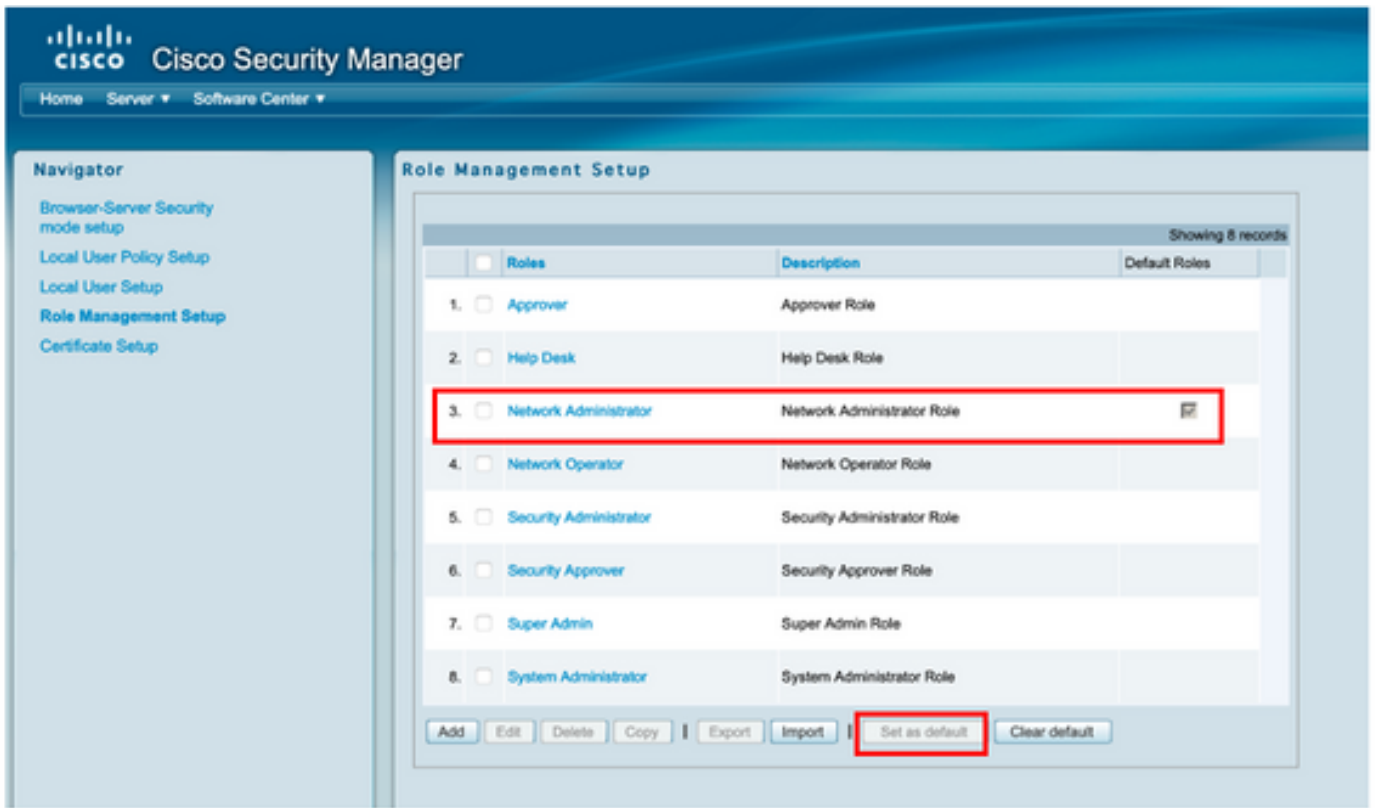
Resource Browser

System Preferences

CS Log Configurations

DiskWatcher Configuration

ステップ7:[Role Management Setup]を選択し、認証時にすべての管理者ユーザが受け取るデフォルトの権限を選択します。この例では、Network Administratorが使用されています。選択したら、既定として**設定**を選択します。

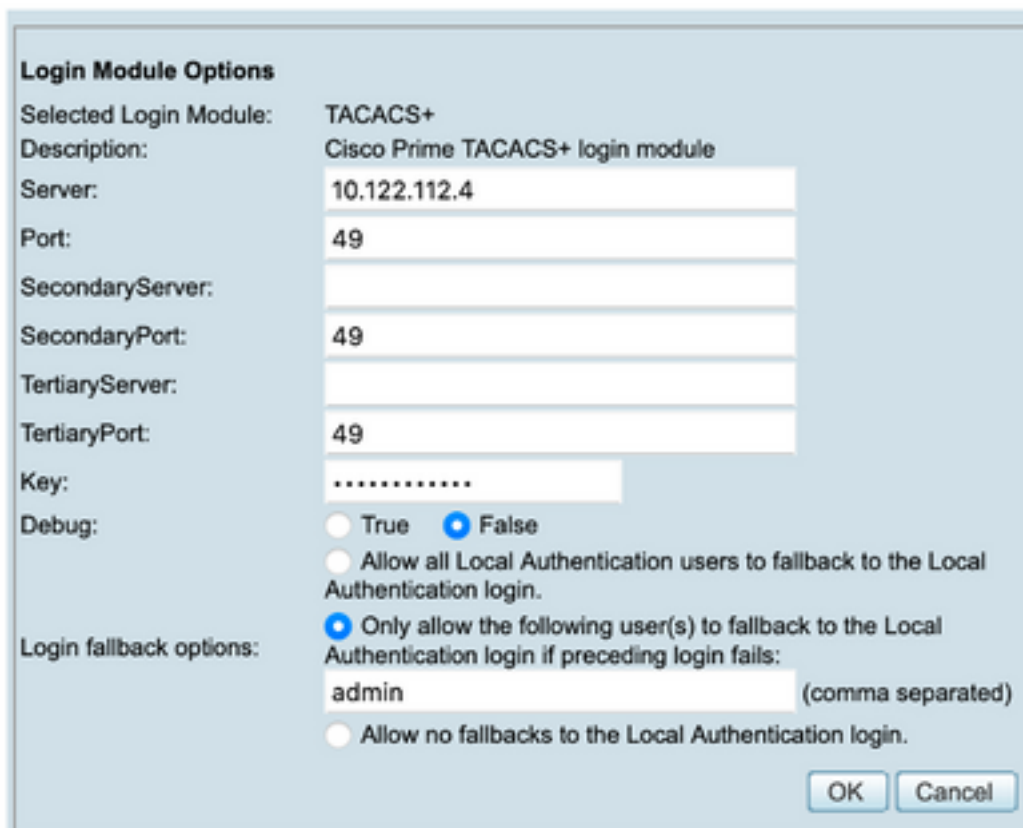


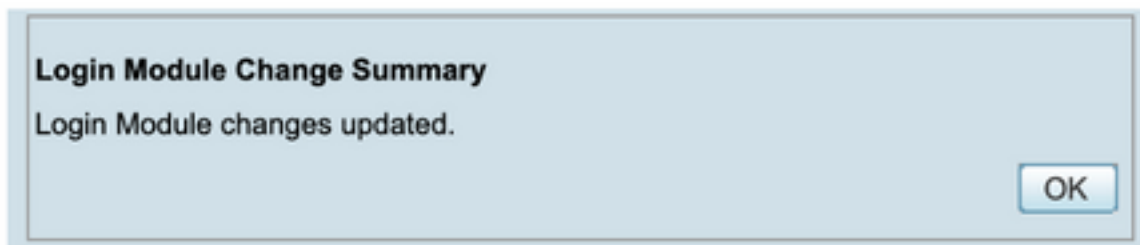
ステップ8:[Sever] > [AAA Mode Setup Role]の順に選択し、[TACACS+]オプションを選択し、最後に[change]を選択してISE情報を追加します。





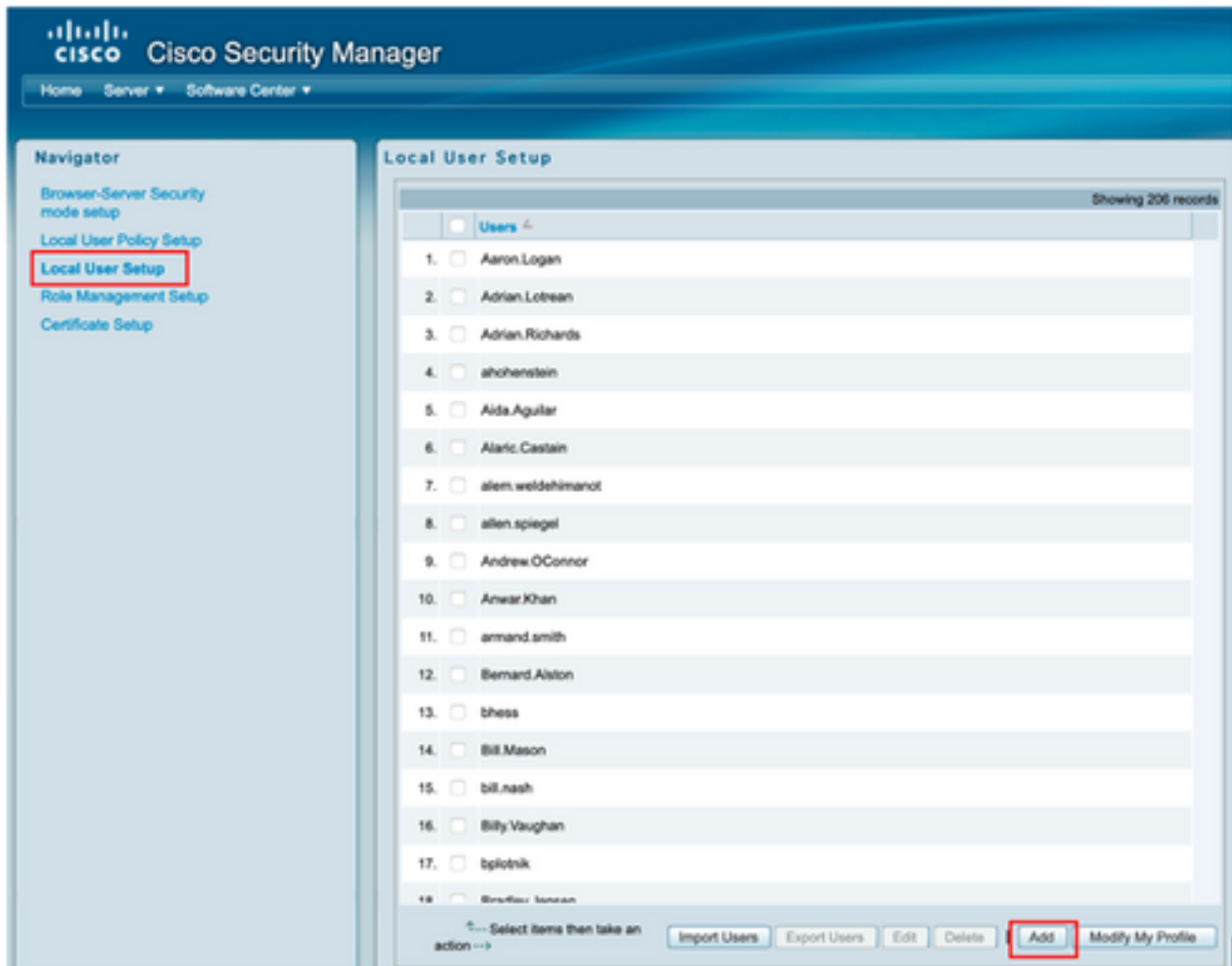
ステップ9: ISE IPアドレスとキーを定義します。オプションで、すべてのローカル認証ユーザを許可するか、ログインに失敗した場合は1人のユーザのみを許可するかを選択できます。この例では、フォールバック方式としてOnly adminユーザが許可されています。[OK]を選択して、変更を保存します。





ステップ10:[Server] > [Single Server Management]を選択し、[Local User Setup]を選択して[add]を選択します。





ステップ11：ステップ5でISEの設定セクションの下に作成した同じユーザ名とパスワードを定義します。この例ではcsmoperとHelp Deskのタスク許可ロールを使用します。[OK]を選択して、管理者ユーザを保存します。

User Information

User Login Details

Username:

Password: Verify Password:

Email:

Authorization Type

Select an option: Full Authorization Enable Task Authorization Enable Device Authorization

Roles

- Help Desk
- Approver
- Network Operator
- Network Administrator
- System Administrator
- Super Admin
- Security Administrator
- Security Approver

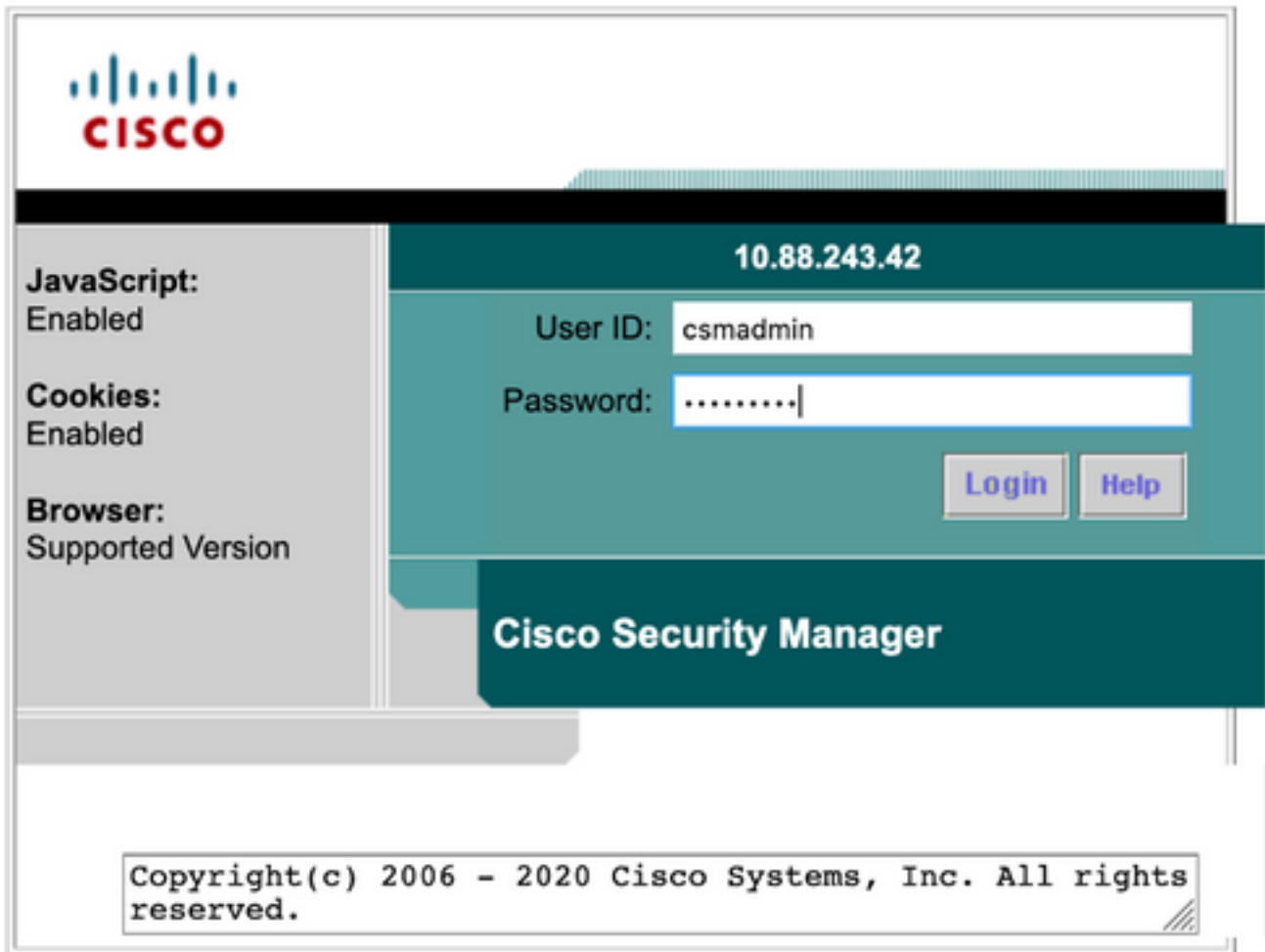
Device level Authorization

Not Applicable

確認

Cisco Security ManagerクライアントUI

ステップ1: 新しいウィンドウブラウザを開き、https://<enter_CSM_IP_Address>と入力し、csmadminのユーザ名とパスワードを使用し、ISE設定セクションのステップ5で作成します。



試行の成功したログインは、ISE TACACSライブログで確認できます

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 02:34:54.1...	Authentic...		csmadmin	Authentic...	CSM 4.22 >> Default		ise30	CSM422

Last Updated: Sat Apr 17 2021 09:37:58 GMT-0500 (Central Daylight Time) Records Shown: 1

Cisco Security Managerクライアントアプリケーション

ステップ1:helpdesk adminアカウントを使用して、Cisco Security Managerクライアントアプリケーションにログインします。



試行の成功したログインは、ISE TACACSライブログで確認できます

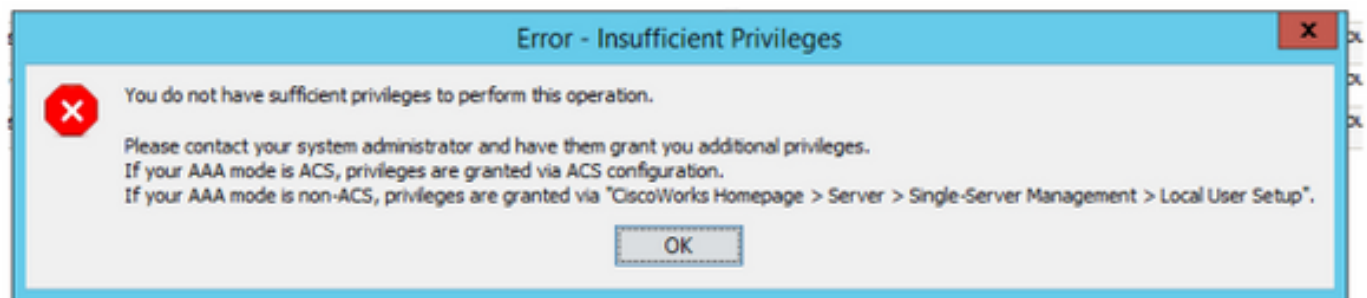
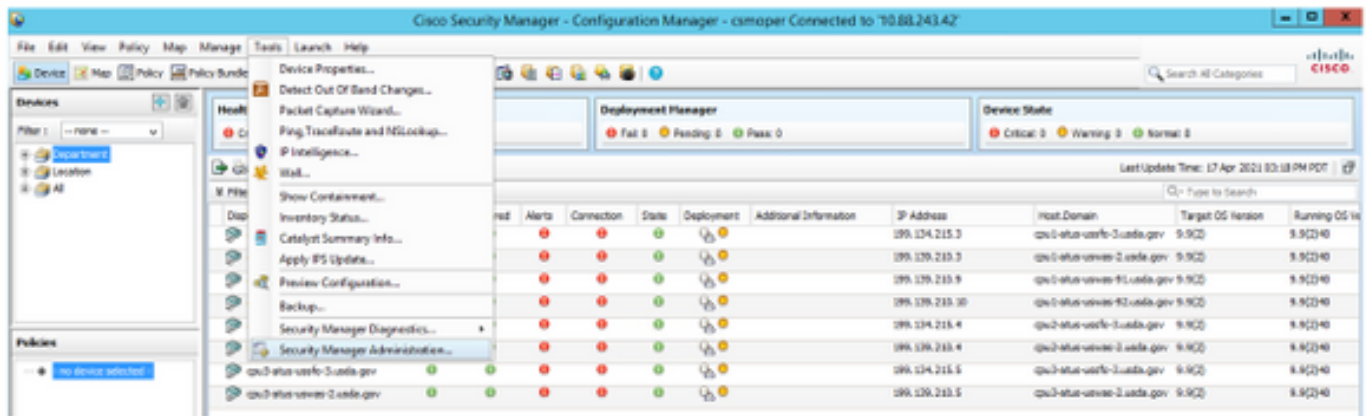
Live Logs

Refresh: Every 3 seconds | Show: Latest 20 records | Within: Last 3 hours

Refresh Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 03:05:58.5...	✓		csmoper	Authentic...	CSM 4.22 >> Default		ise30	CSM422

ステップ2:CSMクライアントアプリケーションメニューから[Tools] > [Security Manager Administration]を選択すると、特権がないことを示すエラーメッセージが表示されます。



ステップ3 : ステップ1から3をcsmadminアカウントで繰り返し、このユーザーに適切な権限が与えられていることを確認します。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

ISEのTCPダンプツールによる通信検証

ステップ1: ISEにログインし、左上にある3つの回線アイコンに移動し、[Operations] > [Troubleshoot] > [Diagnostic Tools]を選択します。

ステップ2: [一般ツール]で[TCPダンプ]を選択し、[Add+]を選択します。[Hostname]、[Network Interface File Name]、[Repository]を選択し、オプションでCSM IPアドレス通信フローのみを収集するフィルタを選択します。[保存して実行]を選択します

Diagnostic Tools Download Logs Debug Wizard

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug
- TCP Dump**
- Session Trace Tests

TrustSec Tools

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name *
ise30

Network Interface *
GigabitEthernet 0

Filter
ip host 10.88.243.42

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
CSM_Tshoot

Repository
VMRepository

File Size
100 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

Promiscuous Mode

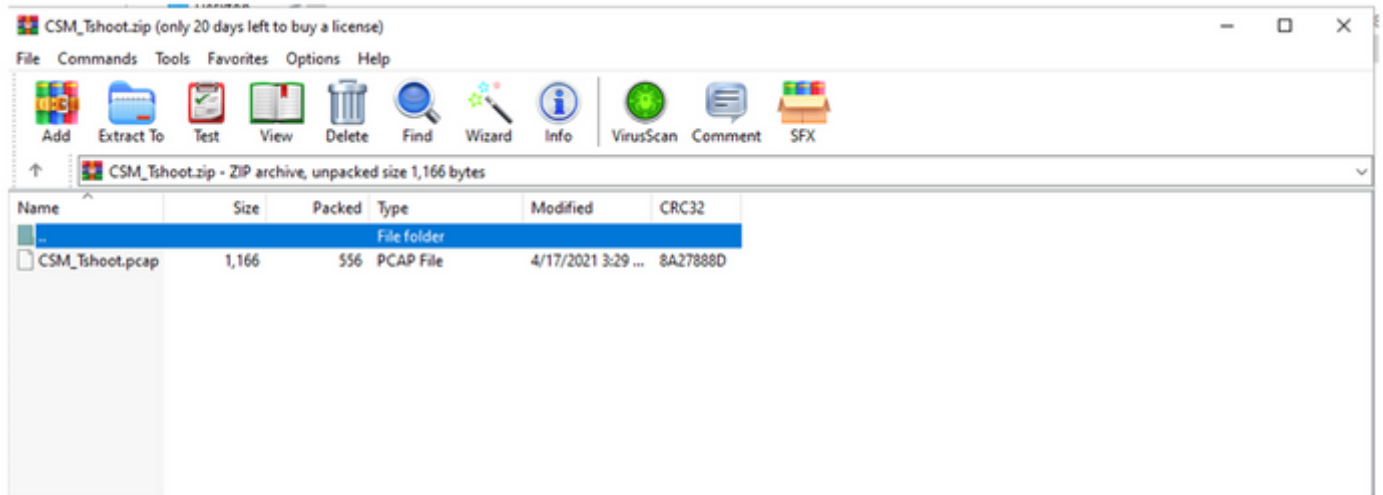
Cancel Save Save and Run

ステップ3: CSMクライアントアプリケーションまたはクライアントUIにログインし、管理者クレデンシャルを入力します。

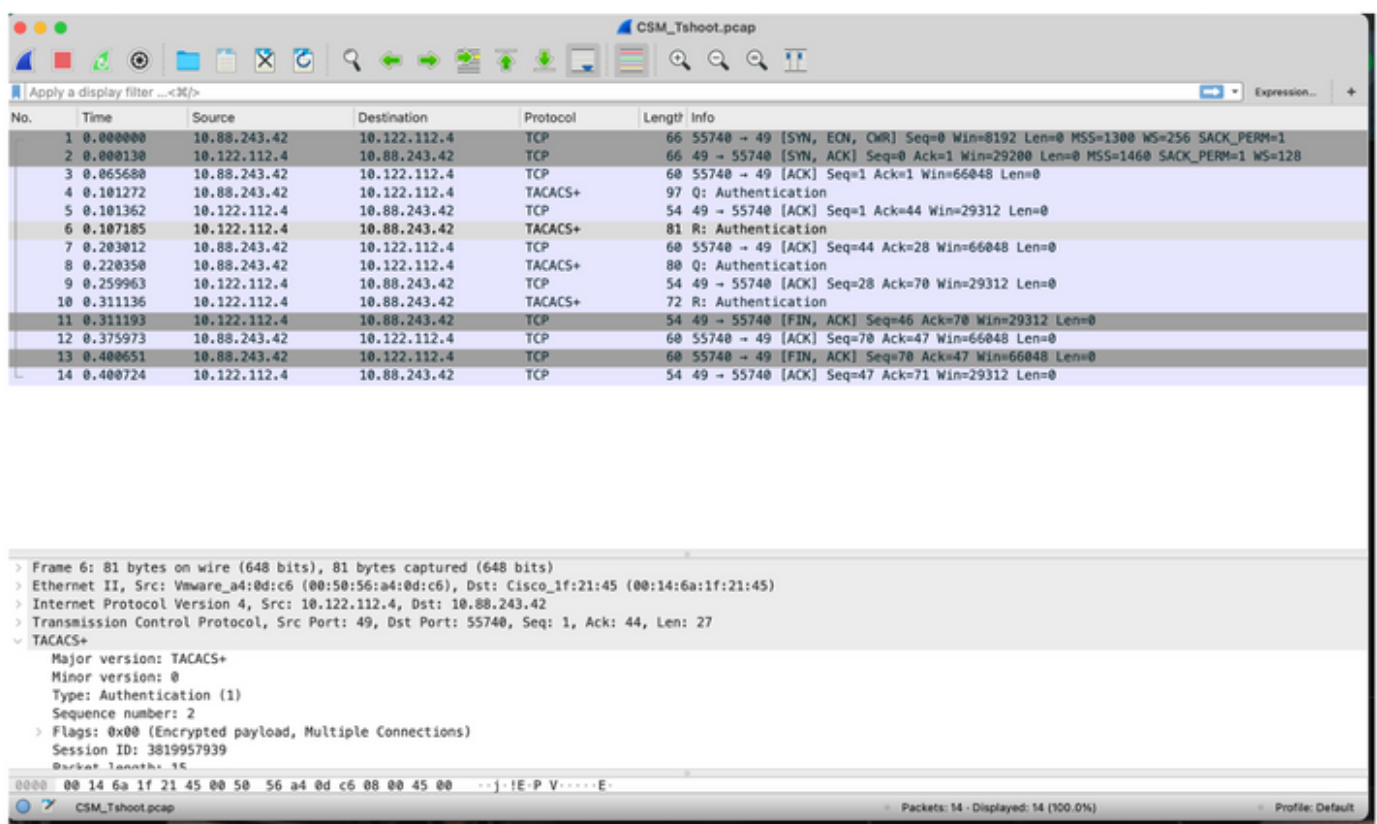
ステップ4: ISEで[Stop]ボタンを選択し、pcapファイルが定義されたリポジトリに送信されたことを確認します。

Refresh + Add Edit Trash Start Stop Download Filter

<input type="checkbox"/>	Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/>	ise30.ciscoise.lab	GigabitEthernet 0	ip host 10.88.243.42	CSM_Tshoot	VMReposit...	100	1



ステップ5:pcapファイルを開き、CSMとISE間の正常な通信を検証します。



pcapファイルにエントリが表示されない場合は、次の点を検証します。

1. ISEノードでデバイス管理サービスが有効になっている
2. CSM設定に正しいISE IPアドレスが追加されている
3. ファイアウォールが中央にある場合は、ポート49(TACACS)が許可されていることを確認します。